PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5553 di Mercoledì 07 febbraio 2024

La sicurezza informatica dei dispositivi medici

Il General Accounting Office ha indagato sulla sicurezza informatica dei dispositivi informatici che permettono di mettere sotto controllo situazioni critiche che coinvolgono i pazienti.

La sanità utilizza sempre più spesso dispositivi informatici, che possono permettere di mettere sotto controllo situazioni critiche, che coinvolgono i pazienti. Come tutti i dispositivi informatici, anche questi possono essere vittime di attacchi cibernetici ed ecco la ragione per la quale il General accounting Office ha condotto uno studio specifico sulla sicurezza informatica di questi apparati.

Se un attacco informatico prende di mira degli apparati medici,

- è possibile che venga compromessa la terapia applicata a pazienti critici,
- è possibile venire a conoscenza di dati particolari afferenti al paziente,
- è possibile impedire o ritardare l'effettuazione di interventi clinici ed infine
- il ripristino può comportare ingenti spese, per recuperare i dati compromessi.

Negli Stati Uniti la Food and Drug Administration-FDA è l'ente federale responsabile per garantire che gli apparati medici, che vengono venduti negli Stati Uniti, offrano soddisfacenti garanzie di protezione da attacchi informatici.

Il General accounting Office è l'ente federale incaricato di esaminare il livello di sicurezza informatica di apparati medici. Per questo motivo nel dicembre 2023 il GAO ha pubblicato un rapporto, che prende in considerazione vari aspetti, soprattutto afferenti al fatto che tutti i prodotti che vengono fabbricati negli Stati Uniti o acquistati all'estero soddisfino a requisiti stringenti, in termini di sicurezza informatica.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[ALDIG02] ?#>

Il GAO ha identificato le agenzie federali, che hanno un ruolo nel garantire la sicurezza informatica degli apparati medici; inoltre lo studio ha preso in esame 25 enti, che rappresentano sia i pazienti, sia i fabbricanti degli apparati medici, sia le strutture sanitarie coinvolte.

Sono state condotte delle interviste con tutti questi enti, in maniera da avere a disposizione un quadro coordinato ed organico della situazione attuale.

Ecco lo schema, in base al quale i criminali possono portare un attacco informatico, diretto a dispositivi medici.



Il criminale ottiene l'accesso alla rete informatica del fabbricante dell'apparato, sfruttando una vulnerabilità del sistema, ad esempio un attacco phishing	Il criminale assume il comando del server al quale, ad esempio, è collegato il monitore cardiaco del paziente.	Effettuando uno scan della rete, il criminale prende il controllo di tutti i monitor cardiaci ed è in grado di disattivarli, esponendo il paziente ad un rischio elevato.	I criminali possono compromettere altri apparati, collegati in rete, aumentando i rischi per i pazienti coinvolti.

Ecco il motivo per cui una legge, pubblicata alla fine del 2022, impone ai fabbricanti di apparati medici, con componenti informatiche, di sottoporre un piano di sicurezza, nel quale devono essere illustrate le caratteristiche di sicurezza del dispositivo e le modalità con cui sia possibile individuare delle vulnerabilità. Purtroppo, questa disposizione legislativa si applica solo a nuovi apparati e non si applica, in maniera retroattiva, agli apparati introdotti sul mercato prima di marzo 2023.

Al termine dell'indagine, il General accounting Office ha avanzato delle raccomandazioni per migliorare le modalità di tempestivo controllo delle caratteristiche di sicurezza informatica di questi dispositivi. La Food and Drug Administration ha condiviso appieno queste raccomandazioni ed ha cominciato ad attivarsi per applicarle al più presto.

Nel frattempo, tutti i soggetti coinvolti sono stati esortati a prestare la massima attenzione a questi problemi. Qualora un lettore si chieda quali analoghe misure siano utilizzate di qua dell'Atlantico, la risposta purtroppo non è soddisfacente!

Adalberto Biasiotti

Licenza Creative Commons